CLAIMS:

1. A method for generating a subscriber identifier, comprising the steps of:

generating an identifier base string based on encrypting a subscriber identifying value;

generating an integrity check value based on the identifier base string; and

generating a subscriber identifier based on a concatenation of the identifier base string and an integrity check value.

2. The method according to claim 1, wherein generating the identifier base string comprises the steps of:

binary coding of the subscriber identifying value,

concatenating a random number, and

performing an encryption algorithm on the concatenated binary coded subscriber identifying value and the random number, for generating the identifier base string.

3. The method according to claim 1, wherein in the subscriber identifier generating step, a base 64 conversion is performed on the concatenated identifier base string and the integrity check value.

4. The method according to claim 1, further comprising the step of using a key indicator for indicating a used ciphering key,

wherein in the identifier base string generating step, the key indicator is concatenated to the value obtained by the encryption of the subscriber identifying value.

5. The method according to claim 2, further comprising the step of using an identifier type indicator for indicating that the subscriber identifier is a particular identifier type, wherein in the identifier base string generating step, the identity type indicator is concatenated to the value obtained by the encryption of the subscriber identifying value.

6. The method according to claim 2, wherein in the performing encryption algorithm step, a defined length is provided for the concatenated binary coded subscriber identifying value and the random number, wherein most significant bits not used for the binary coded subscriber identifying value are set to 1, respectively.

7. The method according to claim 1, wherein the integrity check value is generated by performing a pseudo random function on the identifier base string using an integrity key.

8. The method according to claim 7, further comprising the step of using a key indicator for indicating a used ciphering key and the integrity key used for generating the integrity check value, wherein the key indicator is concatenated to a value obtained by encryption of the subscriber identifying value.

9. The method according to claim 7, wherein the pseudo random function is a keyed hash function.

10. The method according to claim 7, wherein a calculated result of performing the pseudo random function is truncated to a predetermined amount of bits.

11. The method according to claim 1, wherein the subscriber identifying value is an International Mobile Subscriber Identity.

12. A method for validating a subscriber identifier, wherein the subscriber identifier comprises a format including at least integrity check values, the method comprising the steps of:

detecting an integrity check value of a received subscriber identifier,

performing an integrity check based on the integrity check value and the subscriber identifier, and

rejecting the subscriber identifier in case the integrity check reveals that the subscriber identifier is not valid.

13. The method according to claim 12, further comprising the step of

decrypting the subscriber identifier in case the integrity check is successful.

14. A network control node for generating a subscriber identifier, the network node comprising:

means for generating an identifier base string based on encrypting a subscriber identifying value;

means for generating an integrity check value based on the identifier base string; and

means for generating a subscriber identifier based on a concatenation of the identifier base string and the integrity check value.

15. The network control node according to claim 14, wherein the identifier base string generating means comprises:

means for binary coding of the subscriber identifying value;

means for concatenating a random number to the binary coded subscriber identifying value; and

means for performing an encryption algorithm on the concatenated binary coded subscriber identifying value and random number, for generating the identifier base string.

16. The network control node according to claim 14, wherein the subscriber identifier generating means is adapted to perform a base 64 conversion on the concatenated identifier base string and the integrity check value.

17. The network control node according to claim 14, wherein the subscriber identifier generating means is adapted to concatenate a key indicator, for indicating a used ciphering key, to a value obtained by the encryption of the subscriber identifying value.

18. The network control node according to claim 14, wherein the subscriber identifier generating means is adapted to concatenate an identifier type indicator, for indicating that the subscriber identifier is a particular identifier type, to a value obtained by the encryption of the subscriber identifying value.

19. The network control node according to claim 15, wherein a defined length is provided for the concatenated binary coded subscriber identifying value and the random number and wherein the encryption algorithm performing means is adapted to set a value of one for the most significant bits not used for the binary coded subscriber identifying value.

20. The network control node according to claim 14, wherein the integrity check value generating means is adapted to perform a pseudo random function on the identifier base string using an integrity key.

21. The network control node according to claim 14, wherein the subscriber identifier generating means is adapted to concatenate a key indicator for indicating a used ciphering key and an integrity key used for generating the integrity check value to a value obtained by the encryption of the subscriber identifying value.

22. The network control node according to claim 20, wherein the pseudo random function is a keyed hash function.

23. The network control node according to claim 20, wherein the integrity check value generating means is adapted to truncate a calculated result of the pseudo random function to a predetermined amount of bits.

24. The network control node according to claim 14, wherein the subscriber identifying value is an International Mobile Subscriber Identity.

25. A network control node for validating a subscriber identifier, wherein the subscriber identifier comprises a format including at least integrity check values, the network control node comprising:

means for detecting an integrity check value of a received subscriber identifier:

means for performing an integrity check based on the integrity check value and the subscriber identifier; and

means for rejecting the subscriber identifier in case the integrity check reveals that the subscriber identifier is not valid.

26. The network control node according to claim 25, further comprising means for decrypting the subscriber identifier in case the integrity check is successful.

27. The network control node according to claim 25, wherein the network control node comprises an AAA (Authentication, Authorization, and Accounting) server.

28. A computer program product stored on a tangible medium, the product comprising software code, when executed by one or more processors, performs the steps of:

generating an identifier base string based on encrypting a subscriber identifying value;

generating an integrity check value based on the identifier base string; and

generating a subscriber identifier based on a concatenation of the identifier base string and an integrity check value.

29. The computer program product according to claim 28, wherein the computer program product comprises distributed components stored in more than one location of a network.

30. The computer program product according to claim 28, wherein said computer program product is directly loadable into the internal memory of a computer.

31. The computer program product according to claim 28, wherein the computer program product comprises a computer-readable medium on which said software code is stored.